

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK
BUFFALO DIVISION**

NICHOLAS MISSEO, on behalf of himself and
all others similarly situated,

Plaintiff,

v.

THE CANNON CORPORATION d/b/a
CANNONDESIGN,

Defendant.

No. 24-6525

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Nicholas Misso (“Plaintiff”), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant The Cannon Corporation d/b/a CannonDesign (“CannonDesign” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel’s investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant’s failure to protect highly sensitive data.
2. Defendant is an architecture, engineering, and design firm with sixteen offices throughout the United States.¹
3. As such, Defendant stores a litany of highly sensitive personal identifiable information (“PII”) about its current and former employees (and their dependents). But Defendant

¹ *About*, CANNONDESIGN, <https://www.cannondesign.com/about> (last visited Aug. 29, 2024); *Contact*, CANNONDESIGN, <https://www.cannondesign.com/contact> (last visited Aug. 29, 2024).

lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”).

4. It is unknown for precisely how long the cybercriminals had access to Defendant’s network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former employees’ (and their dependents’) PII.

5. On information and belief, cybercriminals were able to breach Defendant’s systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class’s PII. In short, Defendant’s failures placed the Class’s PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice. He brings this class action on behalf of himself, and all others harmed by Defendant’s misconduct.

7. The exposure of one’s PII to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees’ (and their dependents’) private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Nicholas Misso, is a natural person and citizen of New York where he intends to remain.

9. Defendant, The Cannon Corporation d/b/a CannonDesign, is a business corporation incorporated in Delaware and with its principal place of business at 50 Fountain Plaza, Buffalo, New York 14202.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant. And there are over 100 putative Class Members.

11. This Court has personal jurisdiction over Defendant because it is headquartered in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

12. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

13. Defendant is an architecture, engineering, and design firm with sixteen offices throughout the United States.²

14. As part of its business, Defendant receives and maintains the PII of thousands of its current and former employees (and their dependents).

15. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

16. Under state and federal law, businesses like Defendant have duties to protect its current and former employees' (and their dependents') PII and to notify them about breaches.

² *About*, CANNONDESIGN, <https://www.cannondesign.com/about> (last visited Aug. 29, 2024); *Contact*, CANNONDESIGN, <https://www.cannondesign.com/contact> (last visited Aug. 29, 2024).

17. Defendant recognizes these duties, declaring in its “Privacy Policy” that:
- a. “CannonDesign is committed to protecting your personal privacy.”
 - b. “Except as stated in this Privacy Statement, we do not sell, transfer or disclose your Personal Information without your prior consent.”
 - c. “We do not share your personal information, including email address, with any third parties who are not our agents or service providers.”
 - d. “We take reasonable precautions to keep your Personal Information including email address secure.”
 - e. “All access to the information we collect is subject to physical, electronic and managerial restrictions to prevent unauthorized modification, access, or misuse.”

Defendant’s Data Breach

18. From January 19, 2023, until January 25, 2023, Defendant was hacked in the Data Breach.³ Defendant admitted that their Data Breach “impact[ed] the security of information related to certain current or former Cannon Design employees and their dependents.”⁴

19. Notably, Defendant only “became aware of suspicious activity in our computer network” on January 25, 2023.⁵ Thus, Defendant was unable to detect (or stop) the Data Breach for six full days.⁶

³ *Notice of Security Incident*, CANNONDESIGN, <https://www.cannondesign.com/cannon-design-notice-of-security-incident> (last visited Aug. 29, 2024).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

20. Worryingly, Defendant already admitted that “certain information was accessed or acquired by the unauthorized third party.”⁷

21. Because of Defendant’s Data Breach, at least the following types of PII were compromised:

- a. names;
- b. dates of birth;
- c. contact information;
- d. Social Security numbers;
- e. Social Insurance numbers;
- f. driver’s license numbers;
- g. state identification numbers; and
- h. passport numbers.⁸

22. In total, Defendant injured at least 13,049 persons—via the exposure of their PII—in the Data Breach. Upon information and belief, these 13,049 persons include its current and former employees (and their dependents).⁹

23. And yet, Defendant waited over until August 19, 2024, before it began notifying the Class—a *full 572 days* after Defendant learned about its Data Breach.¹⁰

⁷ *Id.*

⁸ *Id.*

⁹ *Data Breach Notifications*, MAINE ATTY GEN, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7574b196-8ba0-439b-a528-be127b9b3a61.html> (last visited Aug. 29, 2024).

¹⁰ *Id.*

24. Stunningly, Defendant admitted that its review of the Data Breach “concluded on May 3, 2024.”¹¹ In other words, Defendant inexplicably delayed notifying the Class for a *full 108 days* after it “concluded” its review.¹²

25. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

26. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

- a. “Cannon Design encourages all potentially impacted individuals to remain vigilant by reviewing account statements, monitoring free credit reports and Explanation of Benefits for suspicious activity, and to detect errors.”¹³
- b. “[O]rder your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.”¹⁴
- c. “[C]ontact the three major credit reporting bureaus listed below to request a free copy of your credit report.”¹⁵
- d. “[E]ducate [yourselves] regarding identity theft, fraud alerts, credit freezes, and the steps [you] can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general.”¹⁶

¹¹ *Notice of Security Incident*, CANNONDESIGN, <https://www.cannondesign.com/cannon-design-notice-of-security-incident> (last visited Aug. 29, 2024).

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

27. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

28. Since the breach, Defendant has declared that “we are working to implement additional security measures[.]”¹⁷ However, such vague statements are insufficient to show that Defendant ***actually implemented*** sufficient data security. Thus, injunctive relief is necessary to ensure that Defendant actually implements sufficient data security.

29. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

30. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

31. Because of Defendant’s Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Avos Locker, Dark Angels, ClubHydra, and the Dark Web

32. Worryingly, the cybercriminals that obtained Plaintiff’s and Class Members’ PII were the cybercriminal group “AvosLocker.”¹⁸ In fact, “a spokesperson [for CannonDesign]

¹⁷ *Id.*

¹⁸ Bill Toulas, *CannonDesign confirms Avos Locker ransomware data breach*, BLEEPING COMPUTER (August 20, 2024, 06:46 PM) <https://www.bleepingcomputer.com/news/security/cannondesign-confirms-avos-locker-ransomware-data-breach/>.

confirmed to BleepingComputer that the disclosure relates to the Avos Locker ransomware attack that occurred early in 2023.”¹⁹

33. AvosLocker is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about AvosLocker.²⁰ Specifically, the joint “Cybersecurity Advisory” (CSA) stated, *inter alia*, that:

- a. “AvosLocker affiliates have compromised organizations across multiple critical infrastructure sectors in the United States, affecting Windows, Linux, and VMware ESXi environments.”²¹
- b. “AvosLocker affiliates compromise organizations’ networks by using legitimate software and open-source remote system administration tools.”²²
- c. “AvosLocker affiliates then use exfiltration-based data extortion tactics with threats of leaking and/or publishing stolen data.”²³

34. Critically, AvosLocker exfiltrated “5.7 TB of stolen data” including the PII of Plaintiff and Class Members.²⁴ Thus far, third-party reports reveal that “the data has been

¹⁹ *Id.*

²⁰ #StopRansomware: AvosLocker, FBI & CISA (Oct. 11, 2023) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a>.

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ Bill Toulas, *CannonDesign confirms Avos Locker ransomware data breach*, BLEEPING COMPUTER (August 20, 2024, 06:46 PM) <https://www.bleepingcomputer.com/news/security/cannondesign-confirms-avos-locker-ransomware-data-breach/> (emphasis added).

published online multiple times and on various sites.”²⁵ A screenshot of AvosLocker’s Dark Web webpage is produced below (albeit redacted to preserve victims’ privacy).²⁶



35. Thereafter, it appears that AvosLocker sold and/or transferred the PII to a different cybercriminal group known as “Dark Angels.”²⁷ Then, third-party reports reveal that Dark Angels “*published* 2TB of data stolen from CannonDesign on September 26, 2023.”²⁸ A screenshot of


²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.* (emphasis added).

Dark Angels' Dark Web webpage (which is called "Dunghill Leak") is produced below (albeit redacted to preserve victims' privacy).²⁹



Dunghill Leak


CannonDesign

September 26, 2023

CannonDesign
<https://www.cannondesign.com>
<https://www.zoominfo.com/c/cannon-design/19714035>

CannonDesign is a global architecture, engineering and consulting practice that provides services for a range of project types, including hospitals and medical centers, corporate headquarters and commercial office buildings, higher education and PK-12 education facilities, hotels and hospitality, mixed-use, sports facilities, and science and research buildings. In 2017 and 2019, Fast Company named CannonDesign one of the 10 most innovative architecture firms in the world.

PREVIOUS LOT: [Robins & Morton](#)



The amount of data reaches 2000 Gb and includes:

- Databases(Argos7, cd-estimating02, cd-cortexsql01, cd-ostakeoff, cd-tipsqprod, cd-intsql01 etc)
- Works
- Projects
- Hiring
- Client Documents
- Marketing
- Quality
- IT-Infrastructure
- etc...

Password for proofs archive: [KJgagUTt8U7h4H7E38H8P7](#)
 Password for all data archives: Will be available soon.

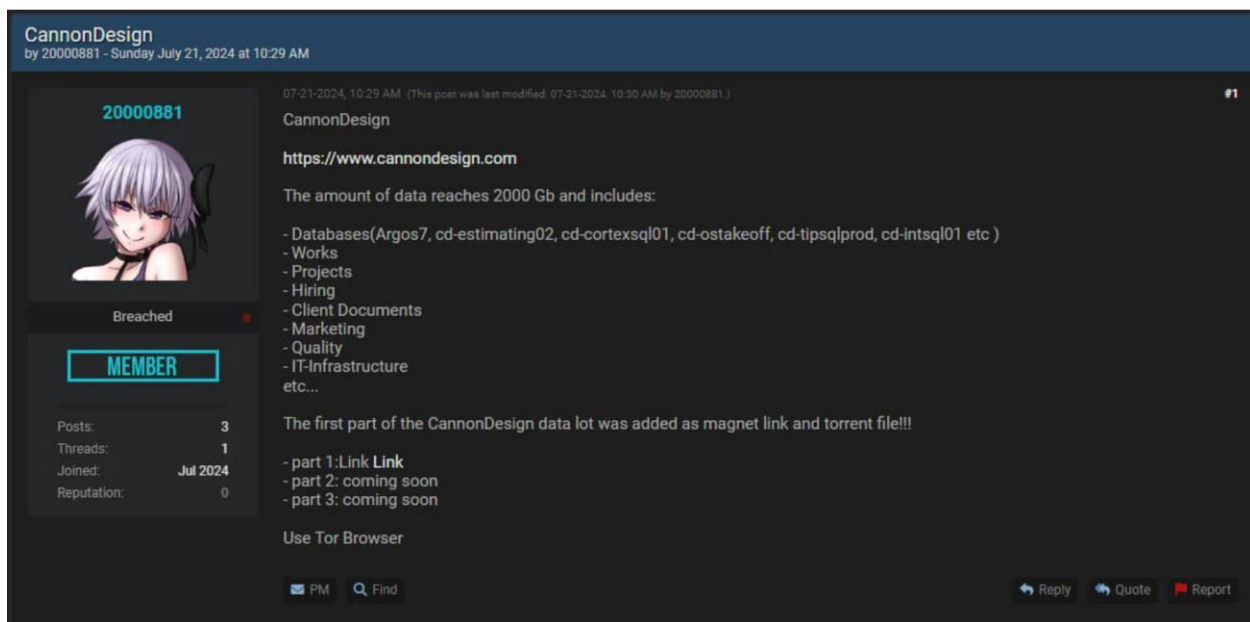
Proofs (1Mb): [Download](#)

Full data (2TB):
 part 1: coming soon
 part 2: coming soon
 part 3: coming soon

²⁹ *Id.*

36. Thereafter, third-party reports reveal that the stolen PII was seemingly sold and/or transferred to the cybercriminal “ClubHydra” and “[i]n February 2024, the same dataset was *published on hacker forums* in the dark web[.]”³⁰

37. And again, on July 21, 2024, the stolen PII was “shared via torrent on Breached Forums in July 2024” with “the data shared freely on clearnet hacking forums[.]”³¹ As such, “the same dataset [] has been circulated online for over a year[.]”³² A screenshot of hacker forum webpage is produced below.³³



38. To make matters worse, in August 2024, in its official data breach notices, Defendant downplayed its Data Breach by declaring that “Cannon Design is *not aware* of any attempted or actual misuse of your information.”³⁴

³⁰ *Id.* (emphasis added).

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ *Data Breach Notifications*, MAINE ATTY GEN, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7574b196-8ba0-439b-a528-be127b9b3a61.html> (last visited Aug. 29, 2024) (emphasis added).

39. However, as detailed *supra*, Defendant “confirmed” that its Data Breach was related to AvosLocker.³⁵ Thus, it appears that Defendant knowingly misrepresented the severity of its Data Breach to Plaintiff and Class Members (i.e., Defendant knew that AvosLocker misused Plaintiff’s and Class Members’ PII and yet falsely declared that it was “not aware” of any such misuse).

40. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII has already been published—or will be published imminently—by Avos Locker, Dark Angels, and/or ClubHydra, on the Dark Web.

Plaintiff’s Experiences and Injuries

41. Plaintiff Nicholas Misso is a former employee of Defendant.

42. Thus, Defendant obtained and maintained Plaintiff’s PII.

43. As a result, Plaintiff was injured by Defendant’s Data Breach.

44. As a condition of his employment with Defendant, Plaintiff provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII in order to obtain employment and payment for that employment.

45. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant’s internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff’s PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

³⁵ Bill Toulas, *CannonDesign confirms Avos Locker ransomware data breach*, BLEEPING COMPUTER (August 20, 2024, 06:46 PM) <https://www.bleepingcomputer.com/news/security/cannondesign-confirms-avos-locker-ransomware-data-breach/>.

46. Plaintiff reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

47. Plaintiff received a Notice of Data Breach in August 2024.

48. Through its Data Breach, Defendant compromised Plaintiff's PII. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

49. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

50. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

51. Indeed, on August 6, 2024, Plaintiff was targeted by cybercriminals when he received an extortionary scam email that:

- a. addressed Plaintiff by his last name "Misso;"
- b. listed Plaintiff's phone number;
- c. claimed to have installed "Malware" on his computer;
- d. claimed to have "gathered all your data;" and
- e. demanded a ransom of \$6950 to be paid in Bitcoin (the ransom letter provided a "BTC ADDRESS" and QR code for Plaintiff to transfer the funds).

52. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

53. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

54. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

55. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

56. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

57. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

58. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII is used;
- b. diminution in value of their PII;
- c. compromise and continuing publication of their PII;

- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII; and
- h. continued risk to their PII—which remains in Defendant’s possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

59. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

60. The value of Plaintiff and Class’s PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the “Dark Web”—further exposing the information.

61. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

62. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

63. The development of “Fullz” packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

64. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members’ stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

65. Defendant disclosed the PII of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

66. Defendant’s failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members’ injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

67. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

68. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.³⁶

69. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”³⁷

70. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

71. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.³⁸ The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;

³⁶ See 2021 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

³⁷ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

³⁸ *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

74. Furthermore, the FTC explains that companies must:

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;
- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

75. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' (and their dependents') data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

77. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

78. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

79. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

81. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

All individuals residing in the United States whose PII was compromised in the Data Breach discovered by CannonDesign in

January 2023, including all those individuals who received notice of the breach.

82. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

83. Plaintiff reserves the right to amend the class definition.

84. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

85. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

86. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 13,049 members.

87. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

88. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

89. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members.

In fact, a class wide proceeding is necessary to answer the following questions:

- a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;
- b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. if Defendant were negligent in maintaining, protecting, and securing PII;
- d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;
- e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. if Defendant's Breach Notice was reasonable;
- g. if the Data Breach caused Plaintiff and the Class injuries;
- h. what the proper damages measure is; and
- i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

90. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would

be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

92. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

93. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

94. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

95. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' PII.

96. Defendant owed—to Plaintiff and Class Members—at least the following duties to:
- a. exercise reasonable care in handling and using the PII in its care and custody;
 - b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
 - c. promptly detect attempts at unauthorized access;
 - d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

97. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

98. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

99. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

100. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

101. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII.

102. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive PII.

103. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

104. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

105. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

106. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

107. Defendant breached these duties as evidenced by the Data Breach.

108. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

- a. disclosing and providing access to this information to third parties and
- b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

109. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

110. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

111. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

112. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

113. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

114. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

115. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

116. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving employment provided by Defendant. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's employment.

117. Plaintiff and Class Members reasonably understood that a portion of the funds derived from their employment would be used to pay for adequate cybersecurity measures.

118. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

119. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

120. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

121. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

122. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

123. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

124. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

125. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

126. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

127. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

128. In these and other ways, Defendant violated its duty of good faith and fair dealing.

129. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

130. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

131. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

133. This claim is pleaded in the alternative to the breach of implied contract claim.

134. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII to facilitate employment, and (2) using their employment to derive profit.

135. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members .

136. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

137. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

138. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

139. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' PII and/or employment because Defendant failed to adequately protect their PII.

140. Plaintiff and Class Members have no adequate remedy at law.

141. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

FOURTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

142. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

143. Plaintiff and Class Members disclosed their highly sensitive PII to Defendant in confidence—with the implicit and explicit understanding that Defendant would collect, store, and protect their PII (and *not* allow the disclosure of their PII to unauthorized third parties).

144. As such, by obtaining (and continuing to maintain) Plaintiff's and Class Members' PII, Defendant assumed an obligation to maintain the confidentiality of that PII.

145. At all times during the relationship between Defendant and Plaintiff and Class Members, Defendant was fully aware of the highly confidential nature of Plaintiff's and Class Members' PII.

146. Thus, Defendant intentionally, knowingly, and/or negligently committed the tort of breach of confidence by, *inter alia*:

- a. failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII;
- b. failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period;
- c. and via the numerous instances of misconduct detailed *supra*.

147. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Violation of New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

150. Section § 349 applies to Defendant because there is a sufficient nexus between Defendant's conduct and New York. After all, Defendant's headquarters is in New York. And

upon information and belief, the deceptive acts or practices discussed herein occurred and/or were authorized in New York.

151. Defendant's deceptive acts and/or practices were directed at consumers because Defendant's privacy policy represented to consumers that it would use reasonable data security. Such representations were deceptive because they induced consumers to disclose their PII.

152. Additionally, Defendant's deceptive acts and/or practices were directed at consumers because Defendant failed to notify consumers about its Data Breach in a reasonable and timely manner. Thereafter, Defendant represented that it was "not aware" of any misuse of Plaintiff's and Class Members PII. Such representation were deceptive because, upon information and belief, Defendant was aware that AvosLocker had *already misused* Plaintiff's and Class Members PII.

153. Furthermore, Defendant violated § 349 by, *inter alia*:

- a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the Data Breach;
- b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e,

and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

- d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and
- e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

154. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

155. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its omissions.

156. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

157. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class Members' rights.

158. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

159. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

160. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

161. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

162. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

163. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

164. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;
- b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;
- c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and
- d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

165. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

166. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

167. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class Members' injuries.

168. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

169. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further unfair and/or deceptive practices;
- E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: September 3, 2024

Respectfully submitted,

By: /s/ James Bilsborrow
James Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
T: (212) 558-5500
jbilsborrow@weitzlux.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class